1) Justifier le passage de $\begin{pmatrix}17\\4\end{pmatrix}$ à $\begin{pmatrix}55\\93\end{pmatrix}$ puis à $\begin{pmatrix}3\\15\end{pmatrix}$.

Déterminons $\begin{pmatrix}y_1\\y_2\end{pmatrix}$

$$C\times\begin{pmatrix}17\\4\end{pmatrix} = \begin{pmatrix}3&1\\5&2\end{pmatrix}\times\begin{pmatrix}17\\4\end{pmatrix} = \begin{pmatrix}3\times17+1\times4\\5\times17+2\times4\end{pmatrix}.$$

$$= \begin{pmatrix}55\\93\end{pmatrix} = \begin{pmatrix}y_1\\y_2\end{pmatrix}.$$

On d'après l'énoncé

$z_1 \equiv 55\ [26]. \iff 55 \equiv z_1\ [26]. \quad 0 \leq z_1 \leq 25$

$55 = 26\times 2 + \boxed{3}. \quad z_1 = 3.$

$z_2 \equiv 93\ [26]$

$93 = 26\times 3 + 15.$ Ainsi $\begin{pmatrix}z_1\\z_2\end{pmatrix} = \begin{pmatrix}3\\15\end{pmatrix}$.

2) Soient x_1, x_2, x'_1, x'_2 quatre nombres entiers compris entre 0 et 25 tels que $\begin{pmatrix}x_1\\x_2\end{pmatrix}$ et $\begin{pmatrix}x'_1\\x'_2\end{pmatrix}$ sont transformés lors du procédé de codage en $\begin{pmatrix}z_1\\z_2\end{pmatrix}$.

a) Montrer que $\begin{cases}3x_1 + x_2 \equiv 3x'_1 + x'_2 \quad (26)\\5x_1 + 2x_2 \equiv 5x'_1 + 2x'_2 \quad (26).\end{cases}$

b) En déduire que $x_1 \equiv x'_1$ (26) et $x_2 \equiv x'_2$ (26) puis que $x_1 = x'_1$ et $x_2 = x'_2$.

a) $\begin{pmatrix}3&1\\5&2\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix} = \begin{pmatrix}3x_1 + x_2\\5x_1 + 2x_2\end{pmatrix}$ $\begin{cases}3x_1 + x_2 \equiv z_1\ [26] \quad (1)\\5x_1 + 2x_2 \equiv z_2\ [26]\end{cases}$

$\begin{cases}(1)\ (a \equiv b\ [c])\\(2)\ (b \equiv d\ [c]).\end{cases}$ $a \equiv d\ [c]$

$$\begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}\begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = \begin{pmatrix} 3x_1' + x_2' \\ 5x_1' + 2x_2' \end{pmatrix} \qquad \begin{cases} 3x_1' + x_2' \equiv z_1 \ [26] \\ 5x_1' + 2x_2' \equiv z_2 \ [26]. \end{cases}$$

Par transitivité, (1) et (2) donnent :

$$\begin{array}{l} (2)\times \\ (-1)\times \end{array}\begin{cases} 3x_1 + x_2 \equiv 3x_1' + x_2' \ (26) \\ 5x_1 + 2x_2 \equiv 5x_1' + 2x_2' \ (26). \end{cases}$$

$a \equiv b \ [c]$
$+$
$(-1)\times (d \equiv e \ [c])$
$a - d \equiv b - e \ [c]$

b) En déduire que $x_1 \equiv x_1' \ (26)$ et $x_2 \equiv x_2' \ (26)$ puis que $x_1 = x_1'$ et $x_2 = x_2'$.

$$\begin{cases} 6x_1 + 2x_2 \equiv 6x_1' + 2x_2' \ [26]. \\ -5x_1 - 2x_2 \equiv -5x_1' - 2x_2' \ [26]. \end{cases}$$

d'où $x_1 \equiv x_1' \ [26]$.

$0 \leq x_1 \leq 25$.

et $0 \leq x_1' \leq 25$.

donc $x_1 = x_1'$.

$a \equiv b \ [c]$.

$c \mid (a-b)$.

$$\begin{array}{l} 5\times \\ 3\times \end{array}\begin{cases} 3x_1 + x_2 \equiv 3x_1' + x_2' \ (26) \\ 5x_1 + 2x_2 \equiv 5x_1' + 2x_2' \ (26). \end{cases}$$

$$\begin{cases} 15x_1 + 5x_2 \equiv 15x_1' + 5x_2' \ [26]. \\ 15x_1 + 6x_2 \equiv 15x_1' + 6x_2' \ [26]. \end{cases}$$

$x_2 \equiv x_2' \ [26]$, or $0 \leq x_2 \leq 25$ et $0 \leq x_2' \leq 25$.

$x_2 - x_2' = 26 \times q \quad q \in \mathbb{Z}$.

$x_2 = 26 \times 9 + x_2'$.

Donc $18 \equiv 14 \ [2]$.

3) On souhaite trouver une méthode de décodage pour le bloc DP :

a) Vérifier que la matrice $\mathbf{C'} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$ est la matrice inverse de $\mathbf{C}$.

$$CC' = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \times \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} = \begin{pmatrix} 3\times 2 + 1\times(-5) & 3\times(-1) + 1\times 3 \\ 5\times 2 + 2\times(-5) & 5\times(-1) + 2\times 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id_2.$$

$$C'C = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \times \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} = \begin{pmatrix} 2\times 3 - 1\times 5 & 2\times 1 - 1\times 2 \\ -5\times 3 + 3\times 5 & -5\times 1 + 3\times 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = Id_2$$

Ainsi C' est l'inverse de C.

b) Calculer $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ tels que $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}\begin{pmatrix} 3 \\ 15 \end{pmatrix}$.

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \times \begin{pmatrix} 3 \\ 15 \end{pmatrix} = \begin{pmatrix} 2\times 3 - 15 \\ -5\times 3 + 3\times 15 \end{pmatrix} = \begin{pmatrix} -9 \\ 30 \end{pmatrix}.$$

$$\begin{cases} -9 \equiv x_1 \ [26] \\ 30 \equiv x_2 \ [26] \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv \boxed{17} \ [26] \\ x_2 \equiv \boxed{4} \ [26] \end{cases}$$

d) On peut conjecturer que pour décrypter un bloc de deux lettres:

1) On trouve les nombres correspondants $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ dans le tableau.

2) On calcule $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ t.q $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = C' \times \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$.

3) On trouve $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ t.q $\begin{cases} x_1 \equiv y_1 \ [26] \\ x_2 \equiv y_2 \ [26] \end{cases}$.

4) Associer $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ aux lettres correspondantes.

4) Dans cette question nous allons généraliser ce procédé de décodage.
On considère un bloc de deux lettres et on appelle z_1 et z_2 les deux entiers compris entre 0 et 25 associés à ces lettres à l'étape 3. On cherche à trouver deux entiers x_1 et x_2 compris entre 0 et 25 qui donnent la matrice colonne $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ par les étapes 2 et 3 du procédé de codage.

Soient y'_1 et y'_2 tels que $\begin{pmatrix} y'_1 \\ y_2 \end{pmatrix} = \mathbf{C}' \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ où $\mathbf{C}' = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$.

Soient x_1 et x_2, les nombres entiers tels que : $\begin{cases} x_1 \equiv y'_1 \ (26) & \text{avec } 0 \leqslant x_1 \leqslant 25 \\ x_2 \equiv y'_2 \ (26) & \text{avec } 0 \leqslant x_2 \leqslant 25 \end{cases}$

Montrer que : $\begin{cases} 3x_1 + x_2 \equiv z_1 \ (26) \\ 5x_1 + 2x_2 \equiv z_2 \ (26). \end{cases}$

Conclure.

$\begin{pmatrix} y_1' \\ y_2' \end{pmatrix} = C' \times \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 2z_1 - z_2 \\ -5z_1 + 3z_2 \end{pmatrix}$.

$\begin{cases} x_1 \equiv y'_1 \ (26) & \text{avec } 0 \leqslant x_1 \leqslant 25 \\ x_2 \equiv y'_2 \ (26) & \text{avec } 0 \leqslant x_2 \leqslant 25 \end{cases}$

$\begin{cases} x_1 \equiv 2z_1 - z_2 \ [26] \\ x_2 \equiv -5z_1 + 3z_2 \ [26]. \end{cases} \Leftrightarrow \begin{cases} 3x_1 \equiv 6z_1 - 3z_2 \ [26] \\ x_2 \equiv -5z_1 + 3z_2 \ [26]. \end{cases}$

$3x_1 + x_2 \equiv z_1 \quad [26]$.

$$\begin{cases} x_1 \equiv 2z_1 - z_2 \ . \ [26] \\ x_2 \equiv -5z_1 + 3z_2 \quad [26] \end{cases} \iff \begin{cases} 5x_1 \equiv 10z_1 - 5z_2 \ [26]. \\ 2x_2 \equiv -10z_1 + 6z_2 \ [26] \end{cases}$$

$$5x_1 + 2x_2 \equiv z_2 \ [26].$$